**REMARKS**

Applicant wishes to thank the Examiner for reviewing the present application.

Applicant also wishes to thank the Examiner for taking the time to participate in the Applicant initiated telephone interview of June 16, 2006. In the telephone interview, the inventiveness of the claims of the present application was discussed, in particular, arguments were presented with respect to the rejections under 35 U.S.C. 103 regarding Schneier in view of Matyas. In summary, it was argued that neither of the references cited by the Examiner recognize the source of the bias discovered by Daniel Bleichenbacher, as the Applicants have recognized, let alone teach choosing a key such that an output not less than $q$ is rejected for use as the key as claimed in the present application. The Examiner suggested that the claims be amended to include linking language for the key and the steps that are used to generate the key, in order to emphasize this distinction and to put the claims in better form for reconsideration.

Applicant believes that the amendments made to claims 1 and 9, described below and outlined above, serve to clarify the nature of the methods claimed and to clearly distinguish over the references cited by the Examiner.

**Claim Amendments**

Claim 1 is amended to identify the key by "*k*", the seed value by "*SV*", and the output by "*H(SV)*".

Claim 1 is also amended inserting "*k* for use in a cryptographic function performed" following "key" on line 1, and inserting the steps "if said output *H(SV)* is rejected, repeating said method; and if said output *H(SV)* is accepted, providing said key *k* for use in performing said cryptographic function, wherein said key *k* is equal to said output *H(SV)*." at the end of the claim.

Claim 9 is amended to identify the key by "*k*", the seed value by "*SV*", and the first output by "*H(SV)*", and the second output by "*H(f(SV))*".

Claim 9 is also amended inserting "*k* for use in a cryptographic function performed" following "key" on line 1, and inserting the steps "if said new output is rejected, repeating said method; and if said new output is accepted, providing said key *k* for use in performing said cryptographic function, wherein said key *k* is equal to said new output." at the end of the claim.

**Claim Rejections**

Claims 1-2 and 4-5 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Matyas. Applicant respectfully traverses the rejections as follows.

The present application describes and claims a method of generating a key that avoids the bias discovered by Daniel Bleichenbacher. Applicant has discovered the source of the bias, namely the way in which the key is chosen. Claim 1, as amended, includes determining if the output (hash of seed value) is less than the order $q$ and if so, the output is accepted as the key. However, if the output is not less than $q$, the output is rejected. Accordingly, the bias is avoided by rejecting the key if not less than $q$. Applicant advises that amended claim 1 includes the steps of repeating the method if the output is rejected and, if the output is accepted, the key $k$ is provided for use in performing the cryptographic function whereby the key $k$ is equal to the output that has been compared to $q$. Applicant believes that these additional steps clearly specify how the key is generated, namely by comparing the output with $q$ until it has a value that is less than $q$.

In previous cryptosystems, e.g. DSS, if the value chosen to be used as the key is greater than $q$ then a mod reduction is performed, which is susceptible to the bias identified by Bleichenbacher. Applicant has recognized the source of the bias and rejects the output instead of performing a reduction to avoid potential attacks. The references relied upon have not recognized this let alone provide any suggestion as to how the bias could be avoided (i.e. the source of the bias). Further, the references cited by the Examiner also do not teach repeating the generation of a seed value and hash thereof until the output is less than $q$ and do not teach providing the output as the key $k$ if the output is less than $q$. Both Schneier and Matyas are entirely silent in that regard.

Therefore, Applicant believes that the amendments made to claim 1 clearly emphasize the above distinction and as such, claims 1-2 and 4-5 are believed to be patentable over the references cited by the Examiner.

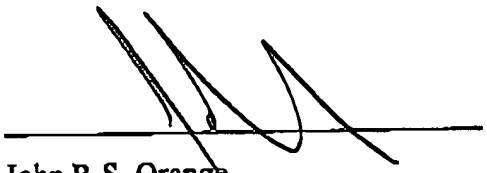
Claims 7-13 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Matyas, in further view of Backal; claims 3 and 6 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Matyas, in further view of Nel; and claim 14 has been rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Backal, in further view of Nel.

As noted above, claim 9 is amended in a manner similar to claim 1 and also includes rejecting an output for use as the key if the output is not less than $q$. Claims 7-8, and 10-14 are ultimately dependent on one of claims 1 and 9. Applicant respectfully submits that neither Backal nor Nel teach rejecting an output for use as the key if the output is not less than $q$. Accordingly, neither Backal nor Nel teach what Applicant is believed to have shown is missing from both Schneier and Matyas. Therefore, for at least that reason, claims 3, 6 and 7-14 are believed to be patentable over the references cited by the Examiner.

In view of the foregoing, Applicant respectfully submits that all pending claims, namely claims 1-14, are patentably distinguished over the references cited by the Examiner and, as such, are in condition for allowance.

Applicant requests early reconsideration and allowance of the present application.

Respectfully submitted,



John R.S. Orange
Agent for Applicant
Registration No. 29,725

Date: 26 July 2006

BLAKE, CASSELS & GRAYDON LLP
Suite 2800, P.O. Box 25
199 Bay Street, Commerce Court West
Toronto, Ontario M5L 1A9
CANADA

Tel: 416.863.3164
JRO/BSL